

REMARKS/ARGUMENTS

Claims 1-10, 16-27, 72, 76-78 and 82-94 were pending in the Office Action. Upon entry of the present paper, claims 6-10, 22-27, 72, 76-78 and 82 are canceled without prejudice or disclaimer, claims 1, 16, 17, 84, 90 and 92 have been amended, and new claims 95-104 are added.

In the Office Action, claims 1-10, 16-27 and 84-94 stand rejected under 35 U.S.C. 102(c) as being anticipated by DeMello et al. (U.S. Patent No. 6,891,953); and claims 90-91 and 93 stand rejected under 35 U.S.C. 103(a) as being unpatentable over an alleged combination of DeMello et al. and Rosen (U.S. Patent No. 5,557,518). Objections to claims 6-10 and 77 were also made, but those objections have been rendered moot by the cancellation of those claims. The remaining rejections are respectfully addressed below.

Independent Claim 1 and Dependent Claims 2-5, 85-89, 92 and 95-98

In rejecting independent claim 1, the Office Action continues to rely on DeMello et al. To show the claimed step of “in response to the request, polling a personal trusted device of said user ...,” the Office Action cites DeMello et al., col. 11, lines 48-55, which discuss the DeMello et al. License Server Module 77. The DeMello et al. License Server Module 77 is part of the Digital Rights Management & Fulfillment Site 73 (see Fig. 4), and is specifically a “sub-component of the download server ISAPI extension DLL 78.” Col. 11, lines 44-45. That fulfillment center provides download services to “a large number of purchasers,” does not belong to the individual purchaser, and is not associated with the individual purchaser. See col. 15, lines 14-15. Instead, the fulfillment center is a separate business that enters into an agreement with the

retailer to handle the downloading of content purchased by the retailer's customers, and even shares a secret symmetric key 75 with the retailer that is not shared with the customers. See, e.g., col. 15, lines 1-47. There is no teaching or suggestion that DeMello et al.'s fulfillment center is a "personal trusted device of said user," as recited in claim 1.

For at least these reasons, Applicants submit that independent claim 1 distinguishes over DeMello et al., and is in condition for allowance. Claims 2-5 and 85-89 depend from claim 1, and are allowable for at least the same reasons as claim 1, and further in view of the various features recited therein. For example, claim 85 recites "[t]he method of claim 1, wherein said personal trusted device is communicatively coupled with said terminal via a wireless interface." Claim 86 goes on to state that "said wireless interface is a low power radio frequency interface." The Office Action cites DeMello et al. Figures 1-4 and col. 5, lines 58-63, but nowhere in those portions (or anywhere else in the patent, for that matter) does DeMello et al. teach or suggest the claimed steps using these recited wireless features. DeMello et al. does mention that its reader can be a PDA, but there is no teaching or suggestion that the PDA uses the recited wireless features as claimed.

The Office Action appears to acknowledge this deficiency, and cites MPEP 2114 as a justification for ignoring the language in this claim. That section, and the Ex Parte Masham case, addresses apparatus claims. Claims 85 and 86 are method claims.

As further examples, newly-added claim 95 recites "wherein said personal trusted device is located proximate to the terminal, and wherein said polling uses a personal area network to instruct said personal trusted device to digitally sign test verification data with a private key of the authorized user stored in said personal trusted device." New claim 98 recites "receiving

polling responses from a plurality of devices located proximate to the terminal and connected to the personal area network.”

Independent Claim 84

Claim 84 was previously dependent from claim 1, and has been rewritten in independent form. The claim includes the recitation “wherein said personal trusted device is a mobile telephone,” and Applicants submit that the cited DeMello et al. reference fails to teach or suggest such a feature. There simply is no teaching or suggestion that the License Server 77, cited by the Office Action to show the claimed personal trusted device, is a mobile telephone. Instead, the server 77 is a software module that is part of the download server 78, and there is no teaching or suggestion in DeMello et al. that the download server 78 is a mobile telephone.

The Office Action also cites MPEP 2114 in this rejection. Again, that section applies to apparatus claims. Claim 84 is a method claim.

Independent Claim 90 and Dependent Claim 91

Claim 90 was previously dependent on claim 1, and has been rewritten in independent form. The claim includes the feature of “randomly generating textual data to be signed by said device.” The Office Action concedes that DeMello et al. fails to teach or suggest such a feature, but cites Rosen (U.S. Patent No. 5,557,518) to address this deficiency. Rosen relates generally to electronic commerce, and involves the use of trusted agent “middlemen” to handle the exchange of money. The Office Action cites the Rosen use of random numbers at Fig. 9b, which

is discussed at col. 16, lines 1-18. There, Rosen uses a random number generator to create a new session key for use in the communications between the middlemen.

Even assuming that DeMello et al. and Rosen are combinable in the first place, the combination would not yield the claim 90 method. Claim 90 recites “polling a personal trusted device of said user to digitally sign said textual data with a private key associated with the device.” When Rosen creates a new session key, it does not use a private key associated with the Session Manager. Instead, it uses the public key of the other server (server B, or the other “middleman”).

Furthermore, there is no logical reason for the alleged combination. The DeMello et al. License Server 77 does not create session keys (DeMello et al. does not mention “sessions” at all), and has no use for the random number session key generation used in Rosen. The Office Action’s alleged motivation, “to have customer communication and authentication in a secure manner by changing the authentication parameters randomly,” is unsupported by the cited art. Nowhere is there any suggestion that randomly changing authentication parameters is somehow desirable to DeMello et al., and Applicants are uncertain as to how that would even work. The prior art must suggest the motivation (MPEP 2143), and in this case, it is apparent that the motivation is not suggested by the prior art, but is rather a hindsight reconstruction motivated by Applicants’ claims.

Independent Claim 16 and Dependent Claims 17-27, 93-94 and 99

Amended independent claim 16 recites, among other features, the following:

a controller configured to:

receive a request to access said stored encrypted content from said licensee of said content;
generate identity verification data in response to said request;
establish, in response to said request, a communication link between the terminal and at least one other local terminal using a personal area network to request the other local terminal to encrypt and digitally sign the identity verification data, generated by said terminal, using a private key stored at the other local terminal and assigned to said licensee of said content;
receive said digitally signed identity verification data from said other local terminal;
use said public key to decrypt said encrypted identity verification data;
analyze said decrypted data to verify that the private key stored at the other local terminal corresponds to the public key in the license, and upon successful verification, decrypt the encrypted content using the content decryption key

None of the cited references, alone or in combination, teaches or suggests the claim 16 terminal with such a controller. For example, the claimed engine is configured to “generate identity verification data” in response to a request to access stored encrypted content, and to “establish, in response to said request, a communication link between the terminal and at least one other local terminal using a personal area network to request the other local terminal to encrypt and digitally sign the identity verification data, generated by said terminal, using a private key stored at the other local terminal and assigned to said licensee of said content.” The DeMello et al. system does not generate such identity verification data and establish such a communication link in response to a request. The Office Action had previously cited the License Server 77 as the other “terminal,” but there is no teaching or suggestion that that License Server 77 stores a private key assigned to a licensee of the content, or uses it to sign identity verification data, as recited. Furthermore, the License Server 77 is not a “local” terminal, but is instead

associated with the download server of the retailer. Additionally, DeMello et al. does not “verify that the private key stored at the other local terminal corresponds to the public key in the license,” as recited.

None of the other cited references teaches or suggests a modification to DeMello et al. that would overcome these deficiencies, and for at least these reasons, amended independent claim 16 distinguishes over the applied references and is in condition for allowance. Claims 17-21, 93-94 and 99 depend from claim 16, and are allowable for at least the same reasons as claim 16, and further in view of the features recited therein. For example, claim 94 recites “wherein said other terminal is a mobile telephone of said licensee.” The Office Action does not cite any mobile telephone teaching from DeMello et al., but instead cites the general DeMello et al. network, and then relies on MPEP 2114 to ignore the mobile telephone language in the claim. MPEP 2114 refers to functional limitations that are recited in certain types of apparatus claims. Claim 94 does not recite any functional limitation. It instead defines the other terminal as a mobile telephone of the licensee. The “mobile telephone” language is part of the claim, cannot be ignored, and the Office Action’s reliance on MPEP 2114 cannot justify the present rejection (which, incidentally, is made under 35 U.S.C. 102).

Independent Claim 100 and Dependent Claims 101-104

New independent claim 100 recites a system that is not taught or suggested by the cited references. For example, claim 100 recites a rendering terminal processor configured to “transmit a polling request to a personal area network local to the terminal, said polling request requesting that a terminal receiving the request digitally sign test verification data using a private

key stored on said terminal, said private key being assigned to said licensee” and “receive a response to the polling request and determine whether said licensee is within a range of said personal area network.” Claims 101-104 depend from claim 100, and are allowable for at least the same reasons as claim 100, and further in view of the features recited therein.

CONCLUSION

All rejections having been addressed, Applicants respectfully submit that pending claims 1-5, 16-21 and 84-104 are in condition for allowance, and respectfully solicit prompt notification of the same. Should the Examiner believe that further discussion and/or amendment would be helpful, the Examiner is invited to telephone Applicants' undersigned representative at the number appearing below.

Respectfully submitted,
BANNER & WITCOFF, LTD.

Date: September 27, 2006

By: /Steve Chang/
Steve S. Chang
Registration No. 42,402

1001 G Street, N.W.
Eleventh Floor
Washington, D.C. 20001-4597
(202) 824-3000